

Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 13.06.2013

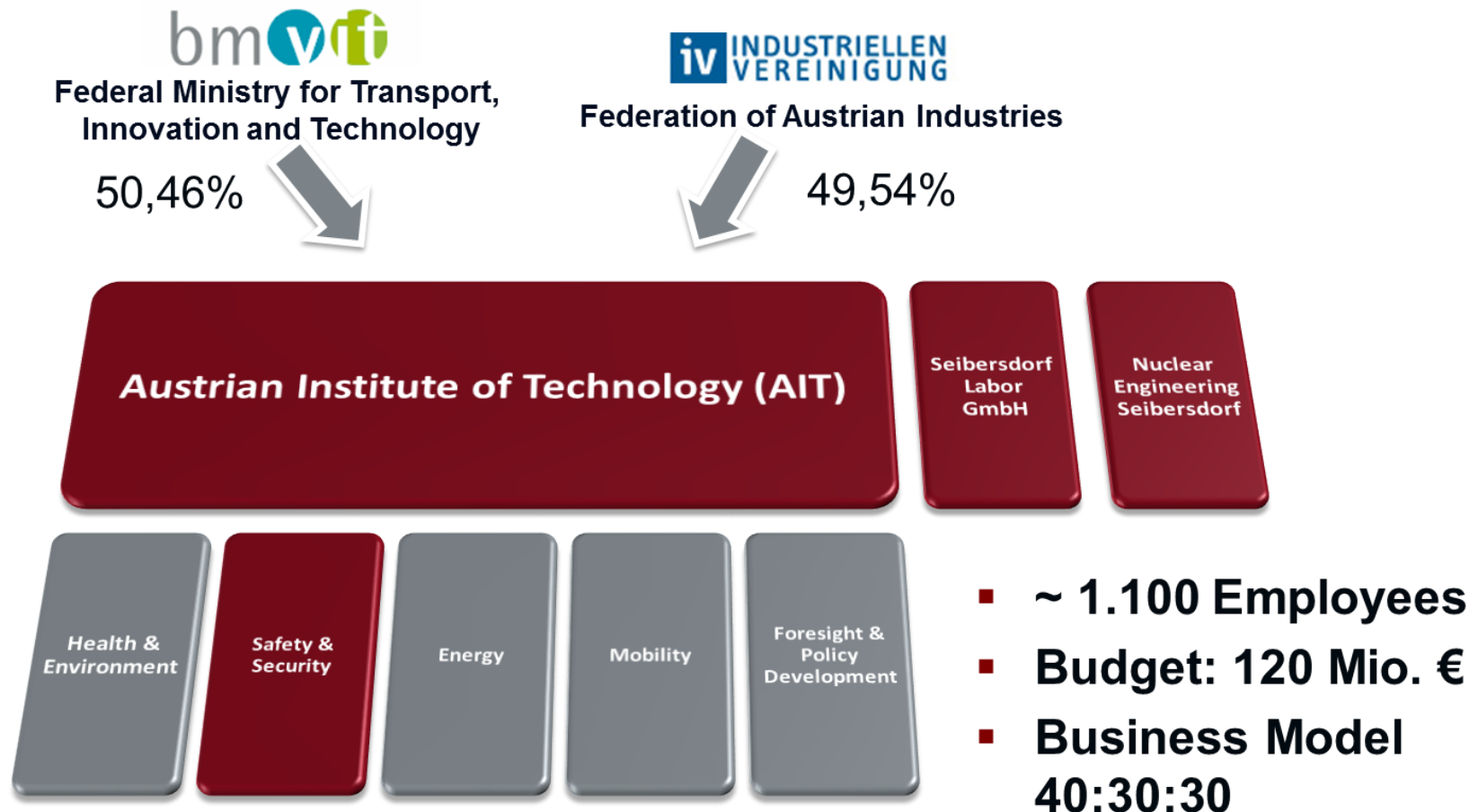
Smart Grid Security in österreichischen Pilotprojekten

Thomas Bleier

AIT Austrian Institute of Technology

AIT Austrian Institute of Technology

- Österreichs größtes außeruniversitäres Forschungszentrum
- Fokussiert auf die Infrastrukturen der Zukunft



Intelligent Vision Systems (IVS)



**Surveillance &
Protection**

*Multi-Camera Vision
High Speed Imaging*

Highly Reliable SW and Systems (HRS)



**Highest System
Reliability**

*Assessment and Testing
of Autonomous and
Safety-Critical Systems*

Future Networks and Services (FNS)



Source: digitalbevaring.dk

**Large Scale Networked
Systems**

*Secure Information Access in
Distributed Systems
Next-Gen. Content
Management Systems
Advanced Applications in
Sensor Networks*

Image Processing

Embedded
Systems & HW
Development

Formal methods

Computer Science & IT
Technologies

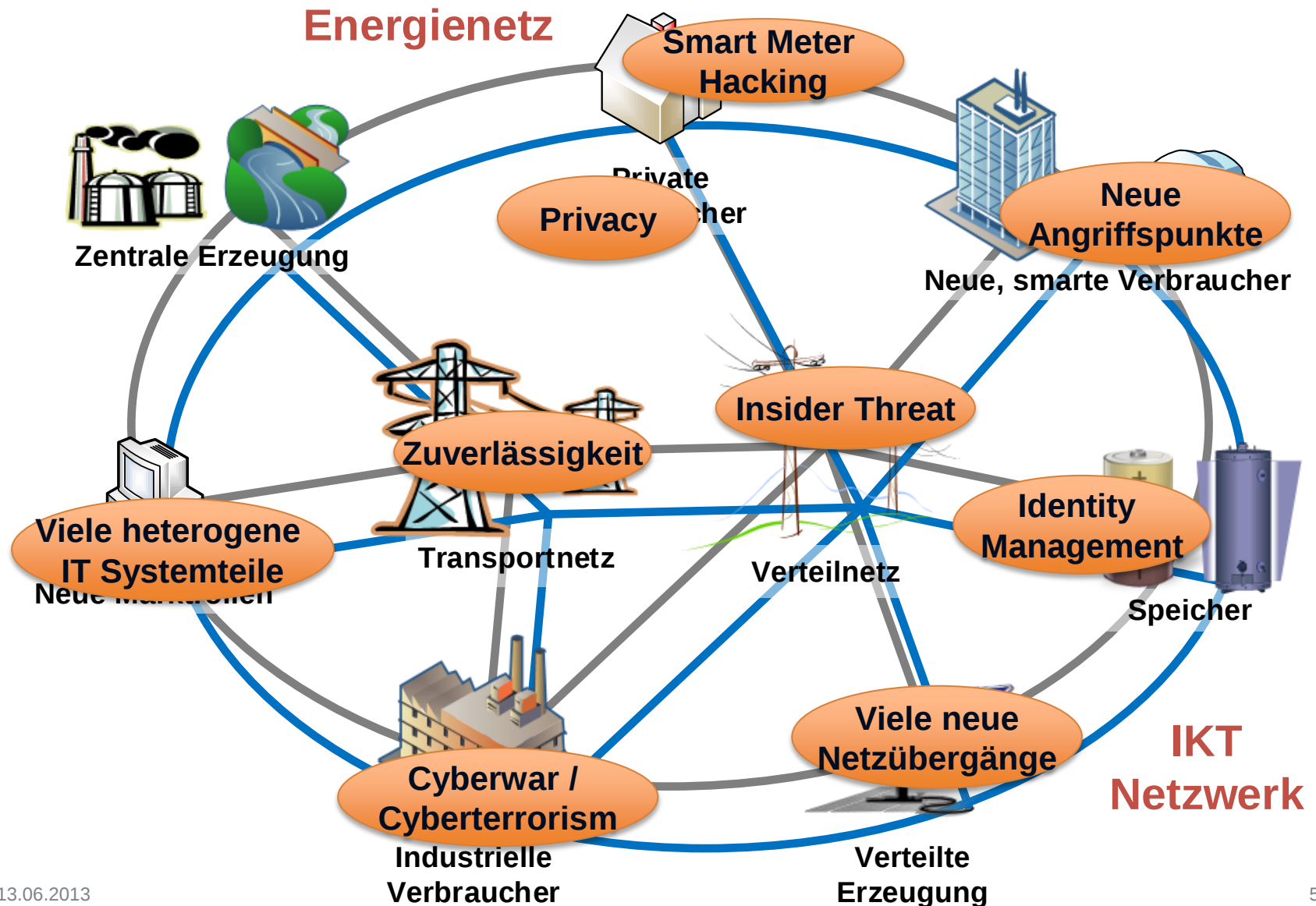
Networking
Technologies

From key scientific competences to focused applied research

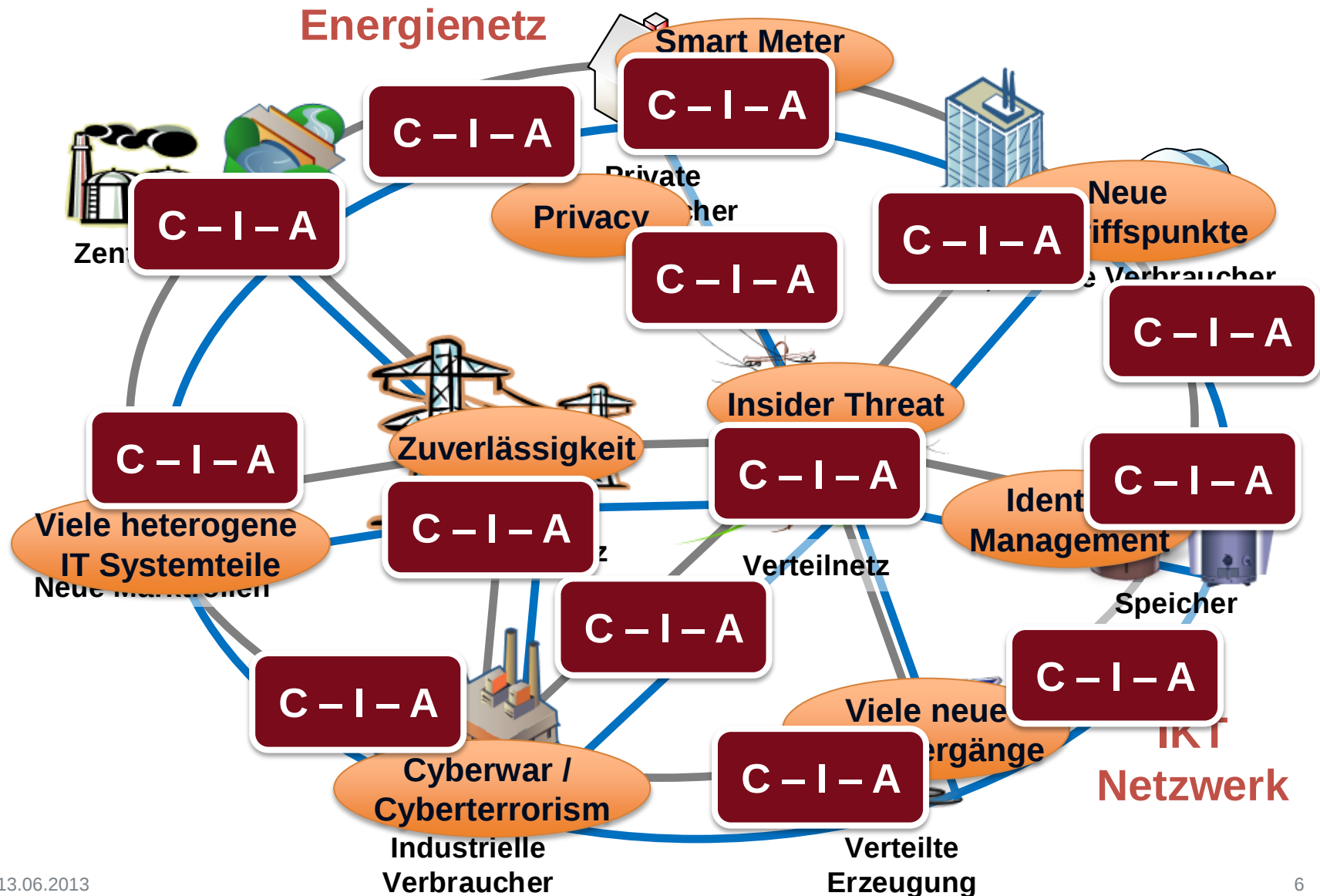
ICT Security Research Programme



Das sichere Smart Grid



Das sichere Smart Grid



IKT-Sicherheitsaspekte im Smart Grid

- Organisatorische Maßnahmen und Sicherheitsprozesse
- Sichere Entwicklung und Inbetriebnahme von Komponenten
- Sicherheit der Kommunikation
- Sicherheit des Betriebes
- Physische Sicherheit
- Behandlung von Sicherheitsvorfällen
- Wiederherstellung im Katastrophenfall

Angelehnt an existierende Standards und Guidelines wie ISO 27002, ENISA
Appropriate security measures for Smart Grids, NIST Guidelines for Smart Grid
Cyber Security, NERC CIP, IEC 62443, etc.

Security-Initiativen und –Projekte im Smart Grid Bereich in Österreich

(SG) ² - Smart Grid Security Guidance	Forschungsprojekt (national)
Integra	Forschungsprojekt (national)
Smart Web Grid	Forschungsprojekt (national)
Österreichs Energie	Verband der E-Wirtschaft
eControl	Energie Regulierungsbehörde
PRECYSE	Forschungsprojekt (EU)
SPARKS	Forschungsprojekt (EU)
HYRIM	Forschungsprojekt (EU)

(SG)² Smart Grid Security Guidance

Projektziele:

- Systematische Erforschung der Sicherheitsaspekte von Smart-Grid-Technologien
 - aufbauend auf existierenden Ansätzen und Ergebnissen
 - unter Berücksichtigung der spezifischen nationalen Gegebenheiten in Österreich
- Erarbeitung von Sicherheitsmaßnahmen für österreichische Energienetzbetreiber
 - Absicherung zukünftiger Energienetze gegenüber IKT-basierten Bedrohungen

Eckdaten (SG)²

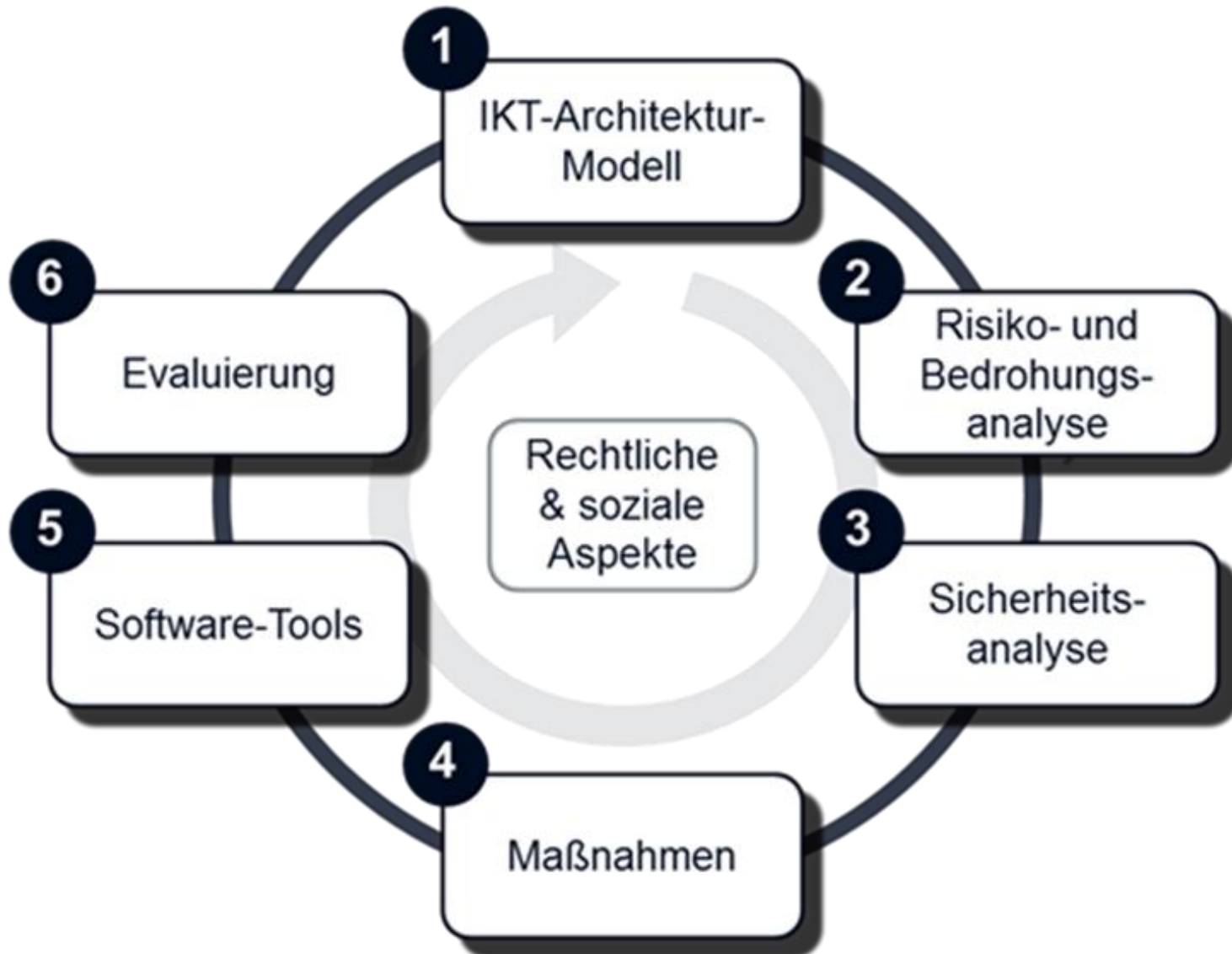
- Nationales Forschungsprojekt im Förderprogramm KIRAS (PL 2.4)
- Laufzeit: 2 Jahre (11/2012 – 10/2014)
- Budget: 1,2 Mio. EUR



- Projektpartner:
 - AIT Austrian Institute of Technology (Koordinator)
 - Technische Universität Wien
 - SECConsult Unternehmensberatung GmbH
 - Siemens AG, Corporate Technology
 - LINZ AG
 - Energie AG
 - Innsbrucker Kommunalbetriebe AG
 - Energieinstitut an der JKU Linz GmbH
 - Bundesministerium für Inneres
 - Bundesministerium für Landesverteidigung



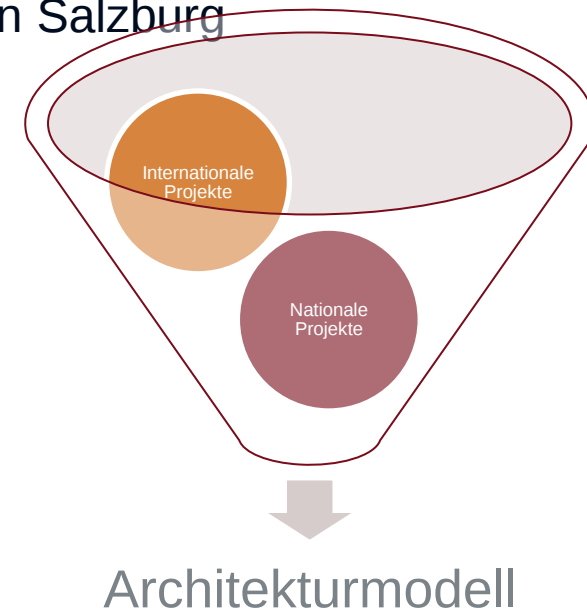
Forschungsthemen & Vorgehensmodell



Definition geeigneter Architekturmodelle (1/3)

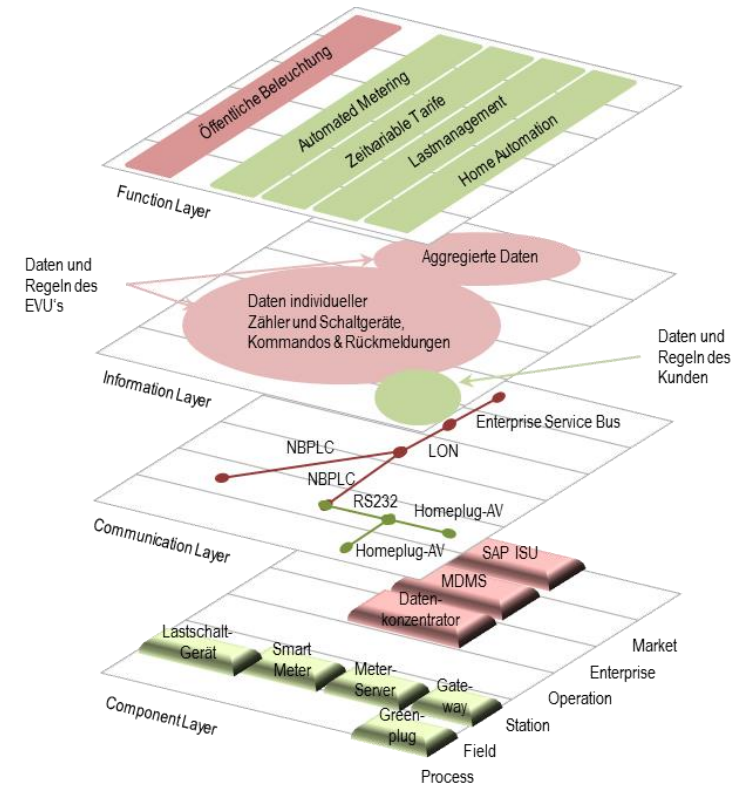
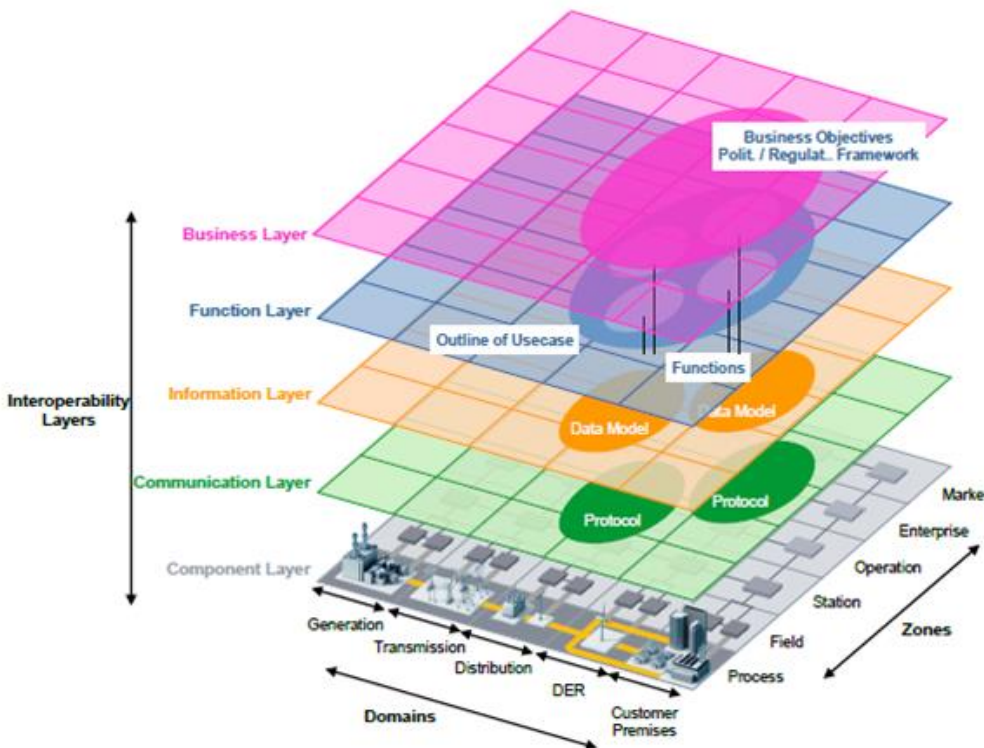
- Analyse relevanter Pilotprojekte
 - IEM: Intelligent Energy Management
 - Smart Web Grid
 - DG DemoNetz Smart LV Grid
 - DG DemoNetz Validierung
 - ZUQDE: Zentrale Spannungs- und Blindleistungsregelung mit dezentralen Einspeisungen in der Demoregion Salzburg
 - EMPORA: E-Mobile Power Austria
 - AMIS Smart Metering Rollout

- OpenNode (EU FP7)
- EcoGrid EU (EU FP7)
- OGEMA (DE)
- Demand Response Automation Server (USA)

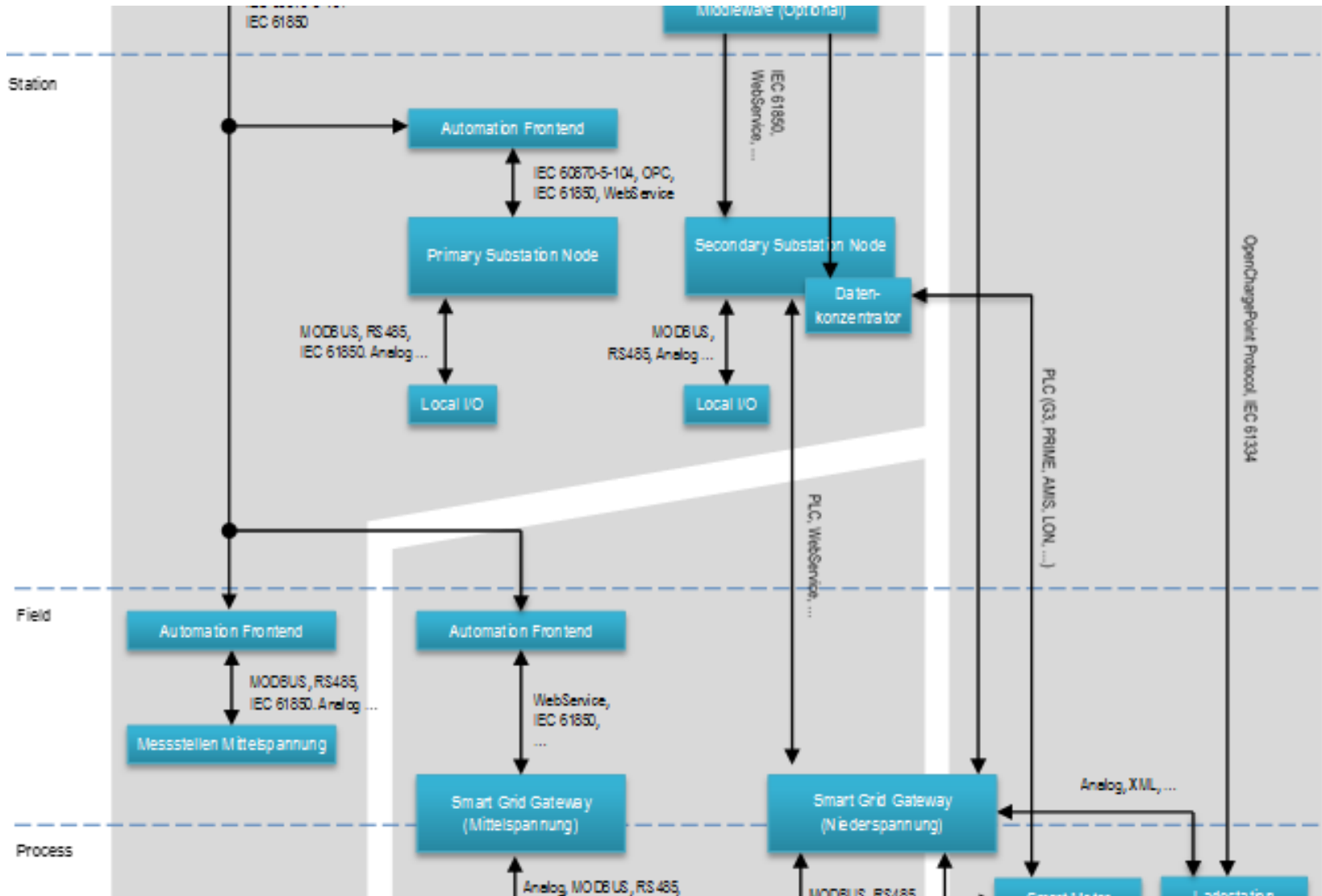


Definition geeigneter Architekturmodelle (2/3)

■ Abbildung der Projektarchitekturen auf SGAM



Definition geeigneter Architekturmodelle (3/3)



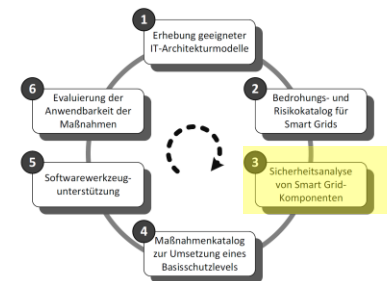
Bedrohungs- und Risikokatalog

- Definition eines Katalogs möglicher Bedrohungen und Risiken im Smart Grid
 - Basis: IT-Grundschutz-Kataloge und Smart Metering Schutzprofil
 - Fokus auf IKT-Aspekte & technische Bedrohungen
- Aus anfangs über 500 Bedrohungen ca. 260 Bedrohungen zur Weiterbetrachtung identifiziert
- Inhaltliche Zusammenfassung ergab **48 Bedrohungen** für den Bedrohungskatalog



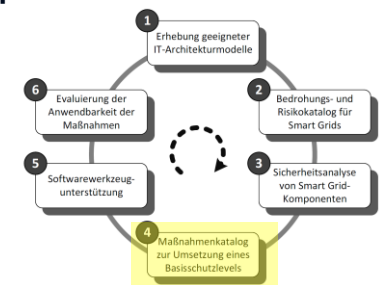
Sicherheitsanalyse von Smart Grid-Komponenten

- Erforschung von aktuellen und zukünftigen Angriffsvektoren
 - für Smart Grid-Infrastrukturkomponenten auf technischer Ebene
- Stichprobenartige Überprüfung ausgewählter Angriffsszenarien
 - in einem Blackbox-Ansatz (d.h. ohne Zusatzinformationen über Komponentendetails wie z.B. Konfiguration und Source Code)
 - in einem Glassbox-Ansatz (d.h. mit Zusatzinformationen)
- Erhebung des aktuellen Sicherheitsniveaus der am Markt befindlichen Produkte
 - mit dem Rückfluss dieser Erkenntnisse in die Produktentwicklung
- Awarenessbildung in Industrie und bei anderen Stakeholdern



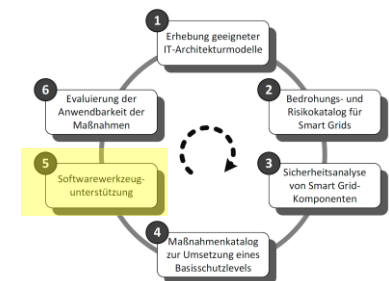
Maßnahmenkatalog zur Umsetzung eines Basisschutzlevels

- Erstellung einer Taxonomie von Angriffen und Gegenmaßnahmen
 - um Attacken und Schutzmaßnahmen strukturiert aufzuarbeiten
- Erarbeitung eines Maßnahmenkatalogs ("Schutzhandbuch")
 - (System, Bedrohung, Risiko)-Kombinationen (Tupel).
 - System und Bedrohung: Informationen über System und potentielle Bedrohungen zur Definition von (techn.) Gegenmaßnahmen,
 - Risiko: Mit einem Risiko wird eine Wahrscheinlichkeit des Auftretens einer Bedrohung assoziiert; speziell unter Berücksichtigung nationaler Gegebenheiten.
- Evaluierung der Schutzmaßnahmen
 - Trennung theoretischer aber wenig praktikabler Konzepte von praktisch besser anwendbaren Maßnahmen
 - Softwaretechnische Unterstützung um eine Konformität mit dem Maßnahmenkatalog zeit- und ressourceneffizient zu erreichen.



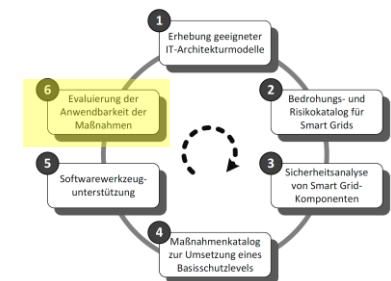
Softwarewerkzeugunterstützung

- Definition von Standarddatenformaten zur Beschreibung
 - von Technologien, Netzwerkkomponenten, Bedrohungen und Sicherheitsmaßnahmen
- Definition von Schnittstellen
 - Für Datenaustausch zwischen verschiedenen Werkzeugen, und Interoperabilität zwischen verschiedenen Instanzen im Bereich Informationssicherheit
- Analyse existierender Ansätze und Werkzeuge
 - und Untersuchung bzgl. Verwendbarkeit und Erweiterbarkeit, z.B. Microsoft Secure Development Lifecycle (SDL), diverse Werkzeuge zur Modellierung von Bedrohungen
- Anpassung existierender bzw. Entwicklung neuer Werkzeuge
 - zur Unterstützung der Umsetzung des Maßnahmenkatalogs



Evaluierung der Anwendbarkeit der Maßnahmen

- Definition von Szenarien
 - (Businessprozesse, Teilsysteme, etc.) für eine aussagekräftige Evaluierung des gesamten Maßnahmenkatalogs
- Anwendung der erarbeiteten Methoden, Techniken, Tools
 - und Entwicklungen in den Pilotszenarien
- Ausarbeitung von konkreten Umsetzungsplänen
 - basierend auf der Anwendung des Maßnahmenkatalogs
- Evaluierung des Sicherheitsgewinns
- Evaluierung der Anwendbarkeit der erarbeiteten Methoden, Techniken und Tools



- Integrierte Smart Grid Referenzarchitektur lokaler intelligenter Verteilnetze und überregionaler virtueller Kraftwerke
- Projektlaufzeit: April 2013 bis Sept. 2015
- Projektpartner:
 - Salzburg AG
 - AIT (Energy)
 - Siemens
 - TU Wien
 - OFFIS
- Ziele:
 - Umsetzung Smart Infrastructure Salzburg
 - Proof of Concept der Missing Links
 - Aktiver, koordinierter Verteilnetzbetrieb, Virtuelles Kraftwerk, Flexibility Operator



INTEGRA - Security

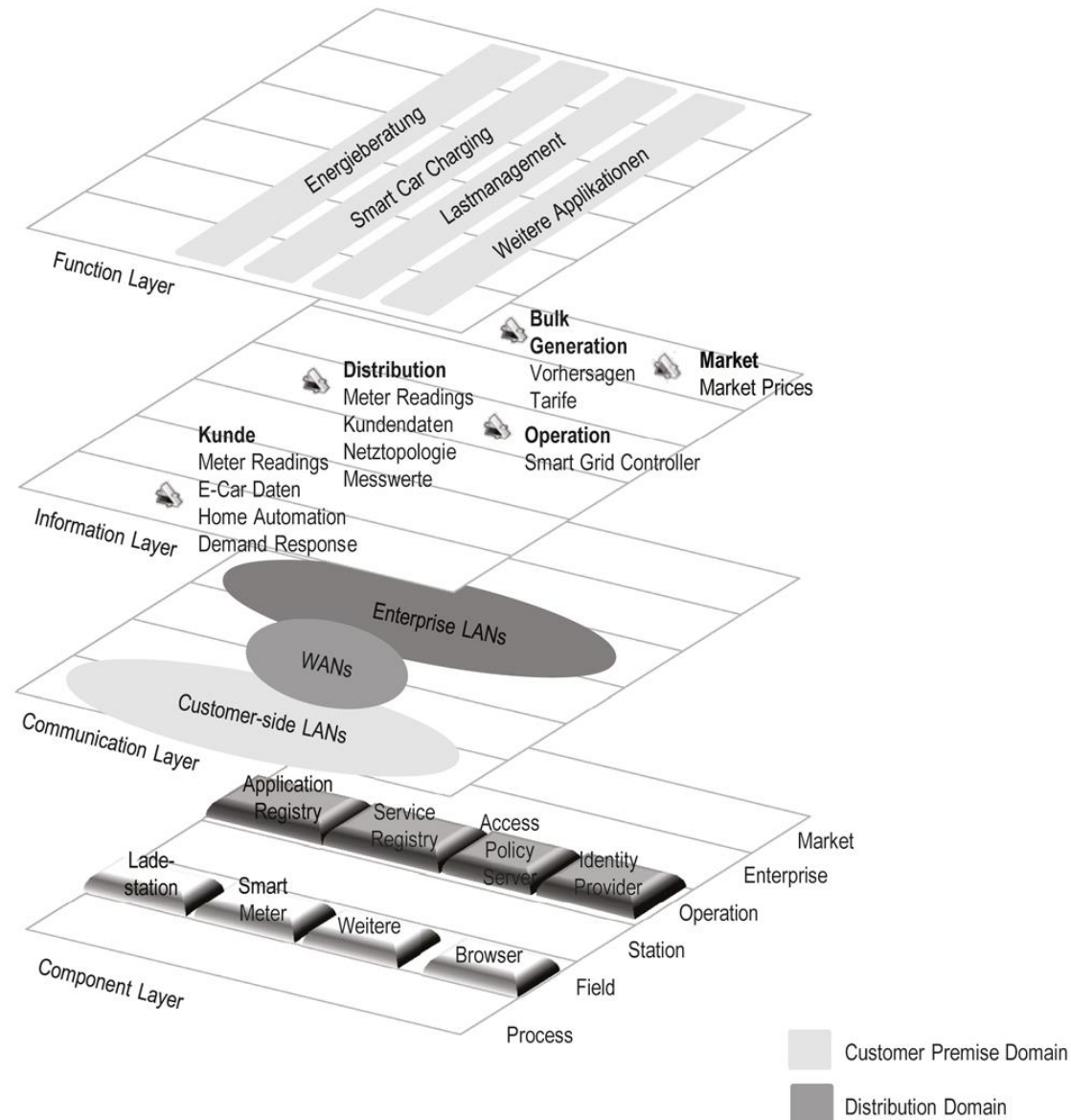
- Fokus auf Security & Privacy – „Security by Design“
- Architektur-Modellierung über UML-basierte Toolbox basierend auf SGAM (M/490)
- Entwicklung von Bewertungs-Metriken
 - Aus State-of-the-Art
 - Auf Basis der Reference Architecture(SGAM)
 - Für Security und Privacy
- Gap-Analyse
 - Anwendung der Metriken auf die SGAM Modelle der einzelnen Projekte
 - Identifikation von Schwachstellen
 - Erstellung eines Maßnahmenkatalogs

Smart Web Grid

- Konzeption eines Informationsmodells für webbasierten Zugriff auf Smart Grids Daten
- Etablierung einer Informationsplattform für Smart Grids für Datenaustausch über einzelne Smart-Grid Anwendungen hinweg
- Projektvolumen: 440 k€, Ausschreibung „Neue Energien 2020“
- Laufzeit: März 2011 bis Juni 2013
- Projektpartner:
 - Salzburg AG
 - Salzburg Wohnbau
 - Siemens
 - AIT (Energy)
 - CURE
 - TU Wien

Smart Web Grid - Security

- Security und Privacy als Designziel von Beginn an (Security by Design)
- Authentifizierung, Rechtemanagement, Policies, etc.
- Auf Basis etablierter Standards (XACML, XAML, X.509, etc.)



- Interessensvertretung der österreichischen E-Wirtschaft
- Projektgruppe „Security im Smart Grid“ – Erarbeitung einer Studie
 - Beschreibung SG aus IKT-Sicht
 - Bedrohungsszenarien beschreiben
 - Analyse der Szenarien & Reihung nach Schadenspotenzial
 - Sicherheitsziele definieren & Gegenmaßnahmen ausarbeiten
 - Handlungsempfehlungen aufzeigen
 - Abschätzung weiterer technologischer Entwicklungen
- Ergebnis sind 90 Handlungsempfehlungen inklusive zeitlicher Handlungsrahmen (kurz/mittel/langfristig) und Durchführung im Einzelunternehmen oder gemeinsam im Verband

- Österreichische Regulierungsbehörde für den Energiemarkt
- Start einer Sicherheitsdiskussion mit Branchenvertretern, Ministerien, Sicherheitsinstitutionen, etc.
- Bericht soll Ende des Jahres 2013 verfügbar sein

Projekt “PRECYSE” – Prevention, protection and reaction to Cyber Attacks to Critical Infrastructures

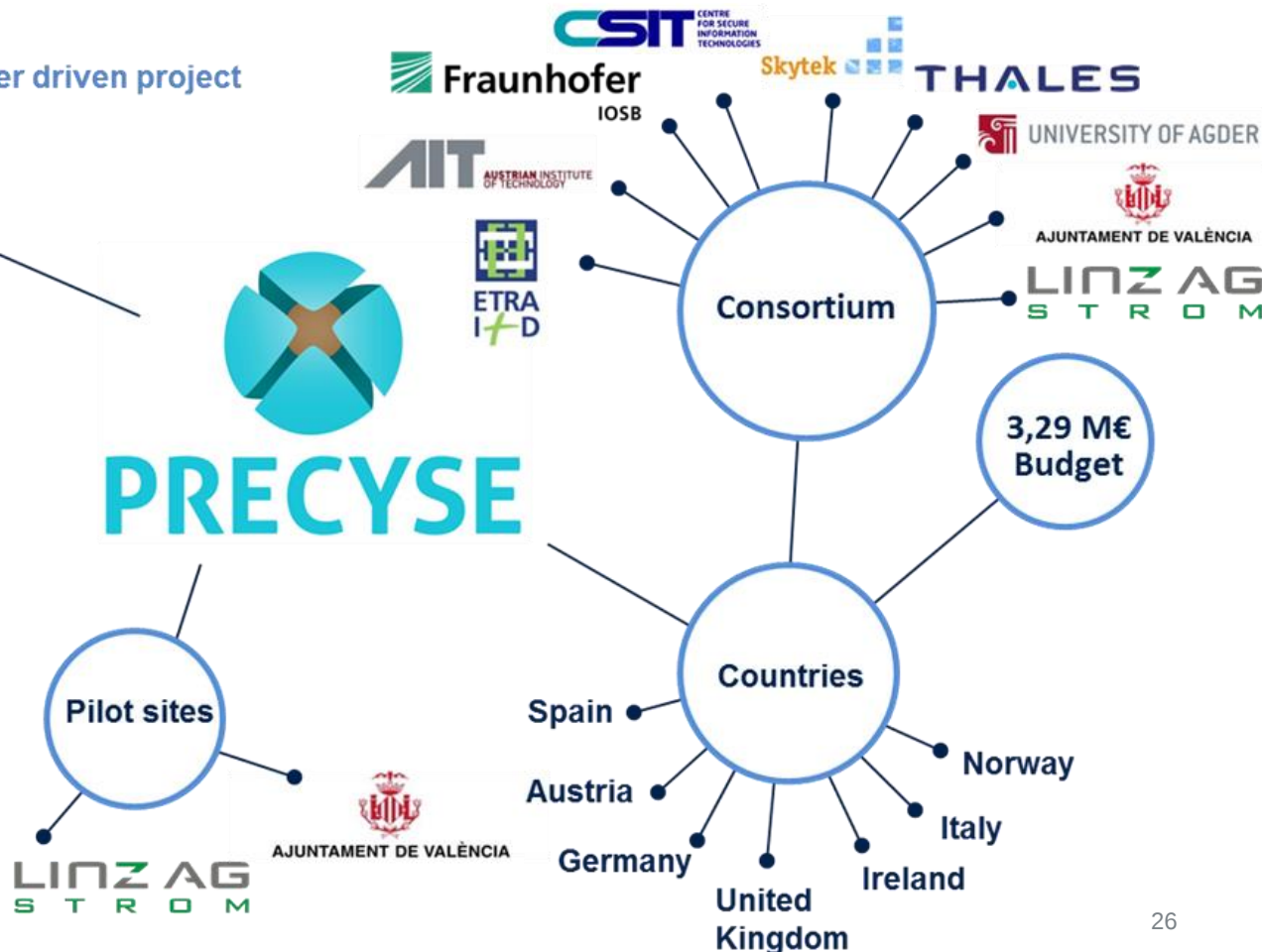
Building on **previous research** and existing standards, and paying attention to relevant **privacy, policy, legal and ethical issues.**

What is PRECYSE?

User driven project

Strategic Goal

Development of a **methodology, an architecture and a set of technologies and tools** to improve –by design– the security, reliability and resilience of the ICT systems supporting Critical Infrastructures



PRECYSE Demonstrationsszenarien

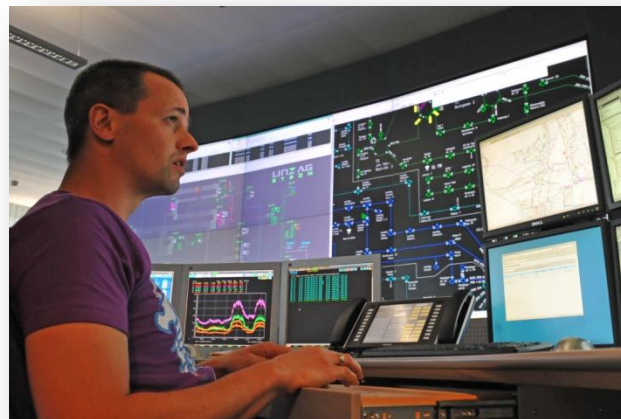


Traffic control centre in the city of Valencia (Spain)

1.5 million inhabitants,
500 000 vehicles

Energy demonstrator in the city of Linz (Austria)

Power supply and related services for 400 000 inhabitants



SPARKS

Smart Grid Protection Against Cyber Attacks



Safety and Security
Department

Energy Department

Foresight & Policy
Development Department

Partner

Fraunhofer
AISEC

**United
Technologies**

**ENERGIE
INSTITUT**
an der Johannes Kepler Universität Linz

CSIT CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES

DIEHL

RSA

KTH
VETENSKAP
OCH KONST

**Landis
Gyr**
manage energy better

HyRiM

Hybrid Risk Management for Utility Providers

- Development and evaluation of risk metrics for interdependent utility network infrastructures to cope with attacks targeted specifically at utility network controls
- Development of tools and methods for risk assessment, which extend existing methodologies towards the handling of new threats (e.g., Advanced Persistent Threats) arising in interdependent utility network infrastructures
- Definition of security architectures to handle threats from emerging technologies, including personal communication devices
- Proposed in the FP7 Security Call 2013



Zusammenfassung

- Verteilte, vernetzte IKT-Systeme sind ein wesentliches, kritisches Element von Smart Grids
- Das Problem ist nicht die Übertragung von existierenden IKT-Sicherheitsproblemen in die Energienetze – durch das Zusammenspiel von IKT und Energienetzen und die Vielzahl der Usecases im Smart Grid entstehen ganz neue Angriffsszenarien und Manipulationsmöglichkeiten
- Sicherheit in solchen Systemen umzusetzen ist schwierig:
 - Viele Beteiligte, keine zentralen Stellen
 - Offene, verteilte Systeme bringen ein höheres Angriffspotential
 - Motivation für Angriffe ändert sich
„Hobby-Hacker“ → Cybercrime → Cyberwar (politisch/militärisch)
 - Methoden für Security Engineering sind in vielen Fällen in der Theorie/im Labor bekannt, werden aber zu oft nicht in der Praxis umgesetzt (zu komplex/teuer, Wissen nicht am richtigen Ort, etc.)

**Adäquate Security ist eine Grundvoraussetzung
für den Erfolg von Smart Grids!**

AIT Austrian Institute of Technology

your ingenious partner

Thomas Bleier

Dipl.-Ing. MSc zPM CISSP CEH

Senior Engineer, Program Manager IT Security

Research Area Future Networks and Services

Safety & Security Department

thomas.bleier@ait.ac.at | +43 664 8251279 | www.ait.ac.at/ict-security